WHAT IS CLAIMED IS:

1. A method for providing security on a computer-network, comprising the steps of:

providing a deception to a network intruder on the computer-network;

monitoring a response of the network intruder to the deception;

detecting the network intruder based upon the response of the network intruder to the deception;

collecting data regarding the network intruder; and

acting on the data regarding the network intruder to protect the computer-network.

2. The method as defined in claim 1, wherein the computer-network is connected to a public network and the deception is accessible via the public network.

3. The method as defined in claim 1, wherein the step of providing a deception the deception is accomplished by emulating an operating system, and wherein the monitoring step monitors attempts by the network intruder to access the emulated operating system.

4. The method as defined in claim 1, wherein the step of providing a deception the deception is accomplished by employing a deceptive machine designation, and wherein the monitoring step monitors attempts by the network intruder to address the deceptive machine designation.

5. The method as defined in claim 1, wherein the step of providing a deception the deception is accomplished by emulating normally protected network processes, and wherein the monitoring step monitors attempts by the network intruder to access the emulated normally protected network processes.

6. The method as defined in claim 1, wherein the step of providing a deception the deception is accomplished by storing deceptive data files with file names selected so

as to attract a network intruder, and wherein the monitoring step monitors attempts by the network intruder to access the deceptive data files.

7. The method as defined in claim 1, wherein the step of providing the deception is accomplished by emulating network equipment or network servers, and wherein the monitoring step monitors attempts by the network intruder to access the emulated network equipment or network servers.

8. The method as defined in claim 7, wherein the emulated network equipment includes at least one selected from the group of network routers, firewalls, Virtual Private Network gateways, and switches.

9. The method as defined in claim 7, wherein the emulated network servers includes at least one selected from the group of Emulating DNS, Intrusion Detection Systems, and Remote Access Server.

10. The method as defined in claim 1, wherein the step of acting on the data regarding the network intruder comprises redirecting the network intruder away from the computer-network.

11. The method as defined in claim 1, wherein the step of acting on the data regarding the network intruder comprises shutting down part or all of the computer-network.

12. The method as defined in claim 1, wherein the step of acting on the data regarding the network intruder comprises informing an operator of the presence of the network intruder via a message.

13. The method as defined in claim 12, wherein the message to the operator is delivered by one or more of the following: a pager message, a telephone call, an e-mail message, an audio alarm and a visual display on a computer monitor.

14. The method as defined in claim 1, wherein the step of acting on the data regarding the network intruder comprises directing a reconnaissance unit on the public web to gather information on the network intruder.

15. The method as defined in claim 1, wherein the step of acting on the data regarding the network intruder comprises storing the data regarding the network intruder in a computer database for later analysis.

16. The method as defined in claim 1, wherein the step of acting on the data regarding the network intruder comprises displaying for an operator the network intruder's actions.

17. The method as defined in claim 1, further comprising the steps of:

intercepting disallowed network activities by the network intruder; and

acting on the intercepted disallowed network activities to protect the computer-network.

18. The method as defined in claim 1, wherein the detecting step comprises detecting a network intruder with a detection unit connected to the computer-network, the detection unit lacking an assigned internet-protocol address.

19. The method as defined in claim 1, further comprising the steps of displaying actions of the network intruder to allow an operator to view the network intruder's actions in real time and provide a direct communication mechanism between the system operator and the intruder.

20. The method as defined in claim 2, further comprising the step of providing data regarding the network intruder to a receiving unit using encrypted protocol data.

21. A method for detecting an intruder on a computer-network with access to a public network comprising the step of:

deceiving the intruder regarding the function, designation or data contents of a deception unit;

gathering data on the intruder as the intruder attempts to access the function, designation or data contents of the deception unit; and

outputting the data on the intruder to a receiving unit.

22. A method for protecting a computer-network once an intruder has been detected, comprising the steps of: .

deceiving the intruder regarding the function, designation or data contents of a deception unit;

permitting the intruder to access the deceptive function, designation or data contents of the deception unit; and

gathering data on the intruder as the intruder accesses the deceptive function, designation or data contents of the deception unit.

23. A method of protecting a computer-network once an intruder has been detected according to claim 20, further comprising the step of redirecting the intruder away from the computer-network.

24. A method of protecting a computer-network once an intruder has been detected according to claim 20, further comprising the step of shutting down all or part of the computer-network.

25. A method of protecting a computer-network once an intruder has been detected according to claim 20, further comprising the step of displaying actions of the network intruder on a watching unit to allow an operator to view the network intruder's actions in real time.

26. A method of protecting a computer-network once an intruder has been detected according to claim 20, further comprising the step of performing reconnaissance on the network intruder using a computer on a public network outside the computer-network.

27. A system for protecting a computer-network connected to a public network from network intruders, comprising:

a management unit;

a sub-network connected to the management unit, the sub-network being separate from the protected computer-network and configured to communicate commands and data to and from the management unit;

a deception unit coupled to the management unit by the sub-network and accessible from the public network;

an interception unit coupled to the computer-network and coupled to the management unit by the sub-network;

a database management unit coupled to the protected computer-network and configured to store data regarding network intruders;

a receiver unit coupled to the management unit by the sub-network and configured to receive data from any one or all of the deception unit, interception unit, and notification unit, and communicate received data to the database management unit for storage; and

a reconnaissance unit coupled to the public network outside the computer-network and coupled to the management unit by the sub-network.

28. The security system according to claim 22, wherein the deception unit runs software stored on read only memory.

29. The security system according to claim 22, further comprising a watching unit coupled to the database management unit and configured to display activities of the network intruder.

30. The security system according to claim 22, wherein the management unit communicates with at least one of the deception unit, notification unit, intercept unit, detection unit, receiving unit, and reconnaissance unit using encrypted protocol data.

31. The security system according to claim 22, further comprising notification unit software stored on a data storage system on a computer coupled to the computer-network, the notification unit software being capable of monitoring activities on the computer to detect suspicious or unauthorized uses of the computer or the computer-network and providing an output to the receiving unit comprising data on the suspicious or unauthorized uses of the computer or the computer-network.

32. A security system for protecting a computer-network connected to a public network from intruders, comprising:

means for deceiving intruders as to the function, designation or content of a machine and providing an output of information regarding intruders' interactions with the means for deceiving, the means for deceiving being coupled to the computer-network and accessible by the public network;

means for detecting intruders based upon information provided in the output of the means for deceiving intruders, the means for detecting intruders being coupled to the computer network and configured to provide an output of data regarding detected intruders;

means for receiving the output of data regarding detected intruders provided by the means for detecting intruders;

means for storing data coupled to the means for receiving the output of data regarding detected intruders; and

means for managing the security system coupled to each of the means for deceiving intruders, detecting intruders, receiving the output of data and storing data.

33. The security system according to claim 32, further comprising:

means for intercepting disallowed network activities by intruders and providing information on the intercepted disallowed activities as an output to the means for receiving the output of data; and

means for monitoring activities on a computer for evidence of intruders and providing the evidence of intruders as an output to the means for receiving output of data.

34. The security system according to claim 32, further comprising:

reconnaissance means for obtaining information on detected intruders, the reconnaissance means being connected to the public network outside the computer-network and coupled to the means for managing the security system.

35. A computer readable data storage medium having program code recorded thereon for the automated detection of a network intruder on a computer-network connected to a public network, the program code comprising:

a first program code that masquerades as a device or network function which the network intruder is likely to seek out, detects the network intruder by monitoring attempts to access the masqueraded device or network function, gathers information on the network intruder and outputs the information on the network intruder;

a second program code that receives the outputted information on the network intruder, and acts upon the outputted information on the network intruder by issuing commands to protect the computer-network; and

a third program code that receives and executes the commands from the second program code.

36. The computer readable data storage medium according to claim 35, wherein the third program code directs the network intruder away from the computer-network.

37. The computer readable data storage medium according to claim 35, wherein the program code executes a shutdown of all or part of the computer-network.

38. The computer readable data storage medium according to claim 35, wherein the program code further comprises:

a fourth program code that monitors activities on a computer for activities that indicate a network intruder, collects data on the activities that indicate a network intruder and provides the collected data to the second program code.

39. The computer readable data storage medium according to claim 35, wherein the program code further comprises:

a fourth program code that manages the operations of the first, second and third program codes.

40. The computer readable data storage medium according to claim 35, wherein the program code further comprises:

a fifth program code under the management of the fourth program code that collects data on the network intruder by monitoring the network intruder message packets and querying the network intruder via the public network.

41. A system for providing security on a computer-network, comprising:

a management component for managing the system;

a deception component for deceiving network intruders and providing an output comprising data on actions taken by the network intruder, the deception component being coupled to the management unit and to the computer network;

a receiving component for receiving the output from the deception component and providing an output of data, the receiving component being coupled to the deception component, and the management component; and

a data collection component for receiving the data output from the receiving component, storing data and providing stored data to the receiving component and/or the management component, the data collection component being coupled to the receiving unit and to the management component.

42. The system according to claim 41, further comprising a watching component for displaying information on the actions of the network intruder, the watching component being coupled to the data collection component and to the management component.

43. The system according to claim 41, further comprising an interception component coupled to the computer-network for intercepting a disallowed use of the computer-network and providing an output to the receiver component comprising data on the disallowed use of the computer-network.

44. The system according to claim 41, further comprising a detection component coupled to the computer-network for detecting disallowed use of the computer-network and providing an output to the receiver component comprising data on the disallowed use of the computer-network, the detecting component lacking an internet protocol address.

45. The system according to claim 41, further comprising a notification component installed on a computer coupled to the computer-network for monitoring the computer for suspicious and disallowed activities and providing an output to the receiver component comprising data regarding suspicious and disallowed activities.

46. A method for providing security for a computer network against network intruders, comprising the steps of:

monitoring the network for intruder activities;

calculating a threat level for the computer network based on the monitored intruder activities ; and

acting on the calculated threat level to protect the computer network.

47. The method according to claim 46, wherein the step of calculating a threat level for the computer network calculates the threat level for the computer network at any given time by weight averaging attacks over a predetermined time window.

48. The method according to claim 46, wherein the step of calculating a threat level for the computer network comprises the further steps of breaking intruder activities into multiple network communication layers, converting the multiple layers into Boolean values and applying the Boolean values in a Boolean logic algorithm to yield an overall threat level.

49. The method according to claim 46, further comprising the step of emulating an entirely virtual network with its own emulated routers and hosts, wherein a deception router unit is assigned to the virtual network to provide deception to network intruders.

50. The method according to claim 46, further comprising the step of providing a secure communication protocol to permit secure communications among all system components.

51. A method for providing security for a computer network against network intruders, comprising the steps of:

monitoring the computer network for an intruder's activities;

providing a visual display of the intruder's activities that permits interaction between the network security operator and the intruder; and

providing a graphical display of the intruder's current activities and historical activities collected over a period of time.

52. The method according to claim 51 further comprises the steps of displaying the intruder's activities as indicia on a radar screen positioned on different sectors of a radar screen having a center and sectors corresponding to different network segments, wherein the proximity of the indicia to the center correlates to a level of threat facing the system.

53. The method according to claim 51, wherein the visual display of the intruder's activities facilitates interactions between security personnel and an attacker.

54. The method according to claim 51 further comprising the steps of an operator conducting a damage assessment using the visual display of the intruders activities; and the operator taking an action to protect the network.